CKN Webinar: 2019-03-05

Trusted Platforms for Critical Infrastructure

Rahul Mavila, Product Manager, IOS XR Security

Dan Backman, Portfolio Architect, SP Automation (Security and Cloud Services)
Speakers

Rahul Mavila  
Product Manager, SP Security  
Cisco

Dan Backman  
Platform Architect, SP Automation  
Cisco
Securing Today’s Service Provider Networks

1. Security and Trust

2. Trust: Enforcement and Reporting

3. Operationalizing Trusted Platform Technologies
Critical Infrastructure Requires Trusted Service Provider Networks
Threat Landscape

Enterprises attacks are mostly robberies

Goal: **Exfiltration**

Attacking SPs is about compromising Critical Infrastructure

Goal: **Turn network into an asset**
“Pwning” Critical Infrastructure

- Denial of Service
- Steering of traffic for surveillance
- Introduce MiTM attacks
  - Malicious DNS Services
  - Compromise trusted services (email or SMS)
- Compromise Telemetry

Threat: Long term compromise to leverage network as an asset
What Is Trust and Why Does It Matter?

To build a trusted platform, network infrastructure must be constructed on a platform of trusted technologies to ensure devices operating are authentic and can create verifiable evidence that they have not been altered.

Secure
Can never be proven and is an ideal state (a goal)

Trust
Can be measured, verified and audited
Security in IOS XR

Protect the IOS XR OS and Platform
- XR Trusted Platform and OS Defenses

Protocol and Platform Hardening
- Protocol Security, Control of external threat surface

IOS XR Security Services
- DDoS Protection, Encryption, and New Revenue Services

- IOS XR as Trusted Platform for Critical Infrastructure
- Securing the IOS XR Threat Surface
- IOS XR as a delivery platform for security services
Trusted Platform

“Integrity, not just security.”
But first, let’s talk a bit about trust & security...
Two primary concepts

Security Controls

Tamper Evidence
Chain of Trust

IOS XR Runtime → Linux Kernel → GRUB Bootloader → BIOS (Firmware) → Processor (Intel?) → Root-of-Trust (Trust Anchor)
Attacking System Integrity

IOS XR Runtime → Linux Kernel → GRUB Bootloader → BIOS (Firmware) → Processor (Intel?)
Cisco Secure Boot vs Standard x86 Solutions

UEFI Secure Boot

Starts at UEFI BIOS

Power On

Bootloader

OS Kernel

HW Anchored Secure Boot

Cisco Root-of-Trust begins in hardware

Power On

Hardware Anchor

CPU Microloader

Bootloader

OS Kernel

© 2019 Cisco and/or its affiliates. All rights reserved
Why Hardware-Anchored Secure Boot Matters


https://blog.f-secure.com/cold-boot-attacks/
Secure boot is a control.

Once it’s complete, how do you know it actually happened?
Would you trust a device to tell you it’s trusted?
Measuring and Validating Trust

Boot & Runtime Measurements

Known Good Values (KGV)

Note: Focus on Known-Good Values. This is not blacklisting.
Secure Quote Process

1) Service requests quote with unique nonce value

2) Router gathers measurements with nonce, creates attestation dossier within signed envelope

3) Service validates:
   - Signature with enrolled key
   - Nonce Value
   - Measurements vs KGVs
Boot Integrity Visibility

Securely measure: hardware, firmware, bootloader, and OS kernel at boot-time.

Must use external service to verify trust

Network Device

Remote Attestation

Integrity Verification

Secure Boot signature check
Integrity measurement

© 2019 Cisco and/or its affiliates. All rights reserved
Extending Trust to Runtime: Process Integrity Validation

Logging

/bin/sh

Appraisal

Trust-Root Certificate in Keyring

PASS: Execution Allowed + Log w/ Signature

FAIL: Execution BLOCKED or WARN

Logging

/bin/sh

Appraisal

Trust-Root Certificate in Keyring

PASS: Execution Allowed + Log w/ Signature

FAIL: Execution BLOCKED or WARN
PoC Demo: IOS XR Process Measurement

Process fingerprint reported by XR Kernel

Hashes of all processes recorded by kernel

(Demo) unauthorized processes identified

© 2019 Cisco and/or its affiliates. All rights reserved
External Validation

Got Trust?
- External service to verify trust
- Collect and sign evidence
- Report and verify that it’s accurate
- Understand the devices being reported on
- Evaluate the evidence versus "known good values"
- Provide insight into the trust posture of the device

Get Benefits
- Evidentiary trail
- Evidence with history
- Unique insights into production systems

Service Provider Threat Landscape  What Is Trust and Why Does It Matter?  External Validation Services
IOS XR Trust:
Trusted Platform Technologies
Cisco Trust Anchor Module (TAm)

HW Root-of-trust and HW Security Module embedded in Cisco Devices

- Secure Boot HW Root
- Strong cryptographic engine
  - Secure Storage for Keys, Certificates, and Objects
- Unique Device Identity
- On each RP, LC, Fabric
Unique hardware Identity (SUDI)

- Unique cryptographic key embedded in hardware trust anchor module within every IOS XR Router
- Secure Unique Device Identifier (SUDI)
- Immutable key imbedded in Trust Anchor Module at time of manufacture
- Signed by Cisco for proof of authenticity
- Validates PID and Serial number of component
- Cryptographically strong identification of remote hardware
- Establishes unique, immutable hardware identity
- Can be used to sign authentication challenges & quotes
Secure Storage of Secrets
What is a secret?

**IOS XR Secrets**
- MACsec pre-shared keys
- SSH Host keys
- Private keys for TLS certificates
- User login password hashes
- Routing protocol authentication strings
- System protocol authentication strings (ntp, snmp, etc)

**3rd Party Applications**
- userID and passwords
- API keys
- TLS keys
Type 6 Encryption

Keys strongly encrypted within IOS XR Configuration

Step 1: Configure master key (AES)

Router (config)# key config-key password-encrypt
New key: *******
Confirm key: *******
Router (config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys with the new master key

Router (config)# key config-key password-encrypt
Old key: *******
New key: *******
Confirm key: Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful

Type 6 service encrypts MACsec PSK Using AES cipher

Router# show running-config key chain kc1
key chain kc1
macsec
  key 1111
    key-string password6
    5d63525a58594657565e6845446842465965554862424c5
    95d696554694a424c59655f504a575e6648484c484b5349675e535a60644e6045654a666858414142
    cryptographic-algorithm aes-128-cmac
    lifetime 00:00:00 january 01 2017 infinite

Master Key in TAm
Hardware Based Secure Storage

Type 6 Master Key

1) User enters cleartext PSK

2) PSK encrypted using master AES key

- Encrypted filesystem to store protected secrets within IOS XR.
- Accessed via TAm services secure storage APIs (internal)

© 2019 Cisco and/or its affiliates. All rights reserved
Expanding Secure Storage

- **TAm Hardware**
- **Hybrid TAm Secure Storage**
  - Encrypted filesystem to stored protected secrets within IOS XR.
  - Accessed via TAm services secure storage APIs (internal)
- **TAm Sync (Secure Replication)**
- **Type 6 Master Key**
  - MACsec PSK
  - Keychain
Cisco Secure Development Lifecycle


- **Plan**: Threat Modeling & Security Requirements
- **Develop**: Secure Modules & Static Analysis
- **Monitor**: Continuous Monitoring & Updates
- **Operate**: Security & Operational Management Process
- **Launch**: Security Release Criteria
- **Validate**: Security Vulnerability Testing

- **Rigorous evolving product security baseline**
- **Minimizes vulnerabilities, enhances security**
- **Embeds security across the portfolio**

© 2019 Cisco and/or its affiliates. All rights reserved
Pervasive Security Strategy

- IP infrastructure: network policy, network slicing, infra protection, traffic steering
- Subscriber services: subscriber id & policy, threat detection, subscriber visibility, content visibility
- Automation: secure deployment, audit & forensics, automated remediation, secure management
- Content & peering: threat detection, encrypted analytics, routing protection, DDoS protection
- SP services: anti-malware, secure SD-WAN, zero-trust networking, SPM/API Security

- Trusted platforms: certified & compliant
- Trusted network infrastructure & automation | Critical & resilient infrastructure
Cisco’s Multi-faceted Approach to Security

Trust & Pervasive Security

**Key Takeaways on Trust**

- Trusted Platforms requires a hardware root-of-trust
- Visibility and Reporting is critical to attest for the integrity of your Trusted infrastructure
- Learn more @ [trust.cisco.com](http://trust.cisco.com)
- Visit [cisco.com/go/sp-trust](http://cisco.com/go/sp-trust)